

Interference & updated Search

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	0	"digital signature".clm. and insert\$3.clm. and "public key".clm. and output\$3.clm. and predetermined.clm. and gps.clm. and authenticat\$3.clm. and bits.clm. and "digital data".clm.	US-PGPUB; USPAT	OR	OFF	2006/12/18 21:02
L2	0	"digital signature".clm. and insert\$3.clm. and "public key".clm. and output\$3.clm. and predetermined\$2.clm. and gps.clm. and authenticat\$3.clm. and bits.clm. and "digital data".clm.	US-PGPUB; USPAT	OR	OFF	2006/12/18 21:03
L3	38	"digital signature" and insert\$3 and "public key" and output\$3 and predetermined\$2 and gps and authenticat\$3 and bits and "digital data"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/12/18 21:04
L4	3330	713/176 or 713/181	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/12/18 21:05
L5	3	4 and 3	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/12/18 21:05


[Subscribe \(Full Service\)](#) [Register \(Limited Service, Free\)](#) [Login](#)

*NPL Search Please
See*

Search: The ACM Digital Library The Guide

"digital signature" and insert\$3 and "public key" and output\$3

SEARCH

THE ACM DIGITAL LIBRARY

[Feedback](#) [Report a problem](#) [Satisfaction survey](#)

Terms used **digital signature** and **insert\$3** and **public key** and **output\$3** and **predetermin\$2** and **gps** and **authenticat\$3** and **bits** and **digital data** Found 286 of 193,448

Sort results by

relevance

[Save results to a Binder](#)

[Try an Advanced Search](#)

Display results

expanded form

[Search Tips](#)

[Try this search in The ACM Guide](#)

Open results in a new window

Results 1 - 20 of 200

Result page: **1** [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [next](#)

Best 200 shown

Relevance scale

1 [On the fly signatures based on factoring](#)



Guillaume Poupard, Jacques Stern

November 1999 **Proceedings of the 6th ACM conference on Computer and communications security**

Publisher: ACM Press

Full text available: [pdf\(786.71 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

In response to the current need for fast, secure and cheap public-key cryptography largely induced by the fast development of electronic commerce, we propose a new on-the fly signature scheme, i.e. a scheme that requires very small on-line work for the signer. It combines provable security based on the factorization problem, short public and secret keys, short transmission and minimal on-line computation. It is the first RSA-like signature scheme that can be used for both ef ...

2 [Network Protocols](#)



Andrew S. Tanenbaum

December 1981 **ACM Computing Surveys (CSUR)**, Volume 13 Issue 4

Publisher: ACM Press

Full text available: [pdf\(3.37 MB\)](#) Additional Information: [full citation](#), [references](#), [citations](#), [index terms](#)

3 [Ad hoc networks: The security of vehicular ad hoc networks](#)



Maxim Raya, Jean-Pierre Hubaux

November 2005 **Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks SASN '05**

Publisher: ACM Press

Full text available: [pdf\(283.96 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

Vehicular networks are likely to become the most relevant form of mobile ad hoc networks. In this paper, we address the security of these networks. We provide a detailed threat analysis and devise an appropriate security architecture. We also describe some major design decisions still to be made, which in some cases have more than mere technical implications. We provide a set of security protocols, we show that they protect privacy and we analyze their robustness, and we carry out a quantitative ...

Keywords: security, vehicular ad hoc networks

4 Architectural support for fast symmetric-key cryptography

 Jerome Burke, John McDonald, Todd Austin
November 2000 **ACM SIGOPS Operating Systems Review , ACM SIGARCH Computer Architecture News , Proceedings of the ninth international conference on Architectural support for programming languages and operating systems ASPLOS-IX**, Volume 34 , 28 Issue 5 , 5

Publisher: ACM Press

Full text available:  pdf(160.25 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

The emergence of the Internet as a trusted medium for commerce and communication has made cryptography an essential component of modern information systems. Cryptography provides the mechanisms necessary to implement accountability, accuracy, and confidentiality in communication. As demands for secure communication bandwidth grow, efficient cryptographic processing will become increasingly vital to good system performance. In this paper, we explore techniques to improve the performance of symmetr ...

5 Protecting digital media content

 Nasir Memon, Ping Wah Wong
July 1998 **Communications of the ACM**, Volume 41 Issue 7

Publisher: ACM Press

Full text available:  pdf(1.02 MB) Additional Information: [full citation](#), [references](#), [citations](#), [index terms](#), [review](#)

6 Cryptographic protocols/ network security: Automatic generation of two-party

 computations
Philip MacKenzie, Alina Oprea, Michael K. Reiter
October 2003 **Proceedings of the 10th ACM conference on Computer and communications security**

Publisher: ACM Press

Full text available:  pdf(238.90 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

We present the design and implementation of a compiler that automatically generates protocols that perform two-party computations. The input to our protocol is the specification of a computation with secret inputs (e.g., a signature algorithm) expressed using operations in the field Z_q of integers modulo a prime q and in the multiplicative subgroup of order q in Z^*p for $q|p-1$ with generator g . The output of our compiler is an implementation of each party in a two ...

Keywords: automatic generation of protocols, secure two-party computation, threshold cryptography

7 Structural digital signature for image authentication: an incidental distortion resistant scheme

 Chun-Shien Lu, Hong-Yuan Mark Liao
November 2000 **Proceedings of the 2000 ACM workshops on Multimedia**

Publisher: ACM Press

Full text available:  pdf(684.69 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

The existing digital data authentication methods are able to detect tampered regions, but are too fragile to resist incidental distortions. This paper will present a new digital signature scheme for image authentication by making use of image content (in the wavelet domain). Based on this concept, a structural digital signature (*SDS*) is constructed. *SDS* is a signature that can be used to judge whether an incoming modification is incidental or malicious. When the structure of an ...

Keywords: authentication, digital signature, fragility, robustness, wavelet transform

8 Security: Ariadne:: a secure on-demand routing protocol for ad hoc networks



Yih-Chun Hu, Adrian Perrig, David B. Johnson

September 2002 **Proceedings of the 8th annual international conference on Mobile computing and networking**

Publisher: ACM Press

Full text available: [pdf\(308.15 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

a secure on-demand routing protocol for ad hoc networks.

Keywords: ad hoc network routing, routing, security



9 Evaluation may be easier than generation (extended abstract)



Moni Naor

July 1996 **Proceedings of the twenty-eighth annual ACM symposium on Theory of computing**

Publisher: ACM Press

Full text available: [pdf\(1.01 MB\)](#) Additional Information: [full citation](#), [references](#), [index terms](#)



10 Computer security (SEC): Fair certified e-mail delivery



Aleksandra Nenadić, Ning Zhang, Stephen Barton

March 2004 **Proceedings of the 2004 ACM symposium on Applied computing**

Publisher: ACM Press

Full text available: [pdf\(179.18 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)



Communication by e-mail has become a vital part of everyday business and has replaced most of the conventional ways of communicating. Important business correspondence may require certified e-mail delivery, analogous to that provided by conventional mail service. This paper presents a novel certified e-mail delivery protocol that provides non-repudiation of origin and non-repudiation of receipt security services to protect communicating parties from each other's false denials that the e-mail has ...

11 Session 3: Detectable byzantine agreement secure against faulty majorities



Matthias Fitzi, Daniel Gottesman, Martin Hirt, Thomas Holenstein, Adam Smith

July 2002 **Proceedings of the twenty-first annual symposium on Principles of distributed computing**

Publisher: ACM Press

Full text available: [pdf\(1.06 MB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#)



It is well-known that n players, connected only by pairwise secure channels, can achieve Byzantine agreement only if the number t of cheaters satisfies $t < n/3$, even with respect to computational security. However, for many applications it is sufficient to achieve *detectable broadcast*. With this primitive, broadcast is only guaranteed when all players are non-faulty ("honest"), but all non-faulty players always reach agreement on whether

broadcast was achiev ...

Keywords: broadcast, byzantine agreement, multi-party computation, public-key infrastructure, quantum signatures

12 Special feature: Report on a working session on security in wireless ad hoc networks

 Levente Buttyán, Jean-Pierre Hubaux
January 2003 **ACM SIGMOBILE Mobile Computing and Communications Review**, Volume 7 Issue 1

Publisher: ACM Press

Full text available: [pdf\(2.50 MB\)](#) Additional Information: [full citation](#), [references](#), [citations](#)



13 Asymmetric fingerprinting for larger collusions

 Birgit Pfitzmann, Michael Waidner
April 1997 **Proceedings of the 4th ACM conference on Computer and communications security**

Publisher: ACM Press

Full text available: [pdf\(1.37 MB\)](#) Additional Information: [full citation](#), [references](#), [citations](#), [index terms](#)



14 A secure multicast protocol with copyright protection

 Hao-hua Chu, Lintian Qiao, Klara Nahrstedt, Hua Wang, Ritesh Jain
April 2002 **ACM SIGCOMM Computer Communication Review**, Volume 32 Issue 2

Publisher: ACM Press

Full text available: [pdf\(301.97 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

We present a simple, efficient, and secure multicast protocol with copyright protection in an open and insecure network environment. There is a wide variety of multimedia applications that can benefit from using our secure multicast protocol, e.g., the commercial pay-per-view video multicast, or highly secure military intelligence video conference. Our secure multicast protocol is designed to achieve the following goals. (1) It can run in any open network environment. It does not rely on any sec ...

Keywords: copyright protection, key distribution, multicast security, watermark

15 Security issues for wireless networks: Two methods of authenticated positioning

 Thomas Mundt
October 2006 **Proceedings of the 2nd ACM international workshop on Quality of service & security for wireless and mobile networks Q2SWinet '06**

Publisher: ACM Press

Full text available: [pdf\(622.43 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

Recent studies and publications have shown a demand for a secure method to proof someones or somenthings position via a communication channel. In this paper we present a concept and two architectures for location dependent access control. We start with a number of scenarios. Some of the scenarios play in a global context, some others in a more local environment. We address boths groups of scenarios with different methods of positioning (location providers). We are using a WLAN mesh network to de ...



Keywords: DRM, MANETs, WLAN positioning, authentication, context/location awareness, mesh networks

16 Session 4: Total recall: are privacy changes inevitable?

 William C. Cheng, Leana Golubchik, David G. Kay
October 2004 **Proceedings of the the 1st ACM workshop on Continuous archival and retrieval of personal experiences**

Publisher: ACM Press

Full text available:  pdf(108.60 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

Total Recall is a system that records an individual perspective of the world using personal sensors such as a microphone in a pair of glasses or a camera in a necklace. There are many applications of Total Recall -- patients accurately recording what they've recently eaten, students replaying any part of a class, and so on--that can significantly improve people's quality of life. However, data recorded by such a system may be also used by the judicial system without the consent of the user or ...

Keywords: personal sensors, privacy, record and playback

17 Bazaars, services, and systems: MoB: a mobile bazaar for wide-area wireless

 Rajiv Chakravorty, Sulabh Agarwal, Suman Banerjee, Ian Pratt
August 2005 **Proceedings of the 11th annual international conference on Mobile computing and networking MobiCom '05**

Publisher: ACM Press

Full text available:  pdf(344.72 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

We introduce MoB, an infrastructure for collaborative wide-area wireless data services. MoB proposes to change the current model of data services in the following fundamental ways: (1) it decouples infrastructure providers from services providers and enables fine-grained competition, (2) it allows service interactions on arbitrary timescales, and, (3) it promotes flexible composition of these fine-grained service interactions based on user and application needs. At the heart of MoB is an open mar ...

Keywords: incentives, reputation, wide-area wireless, wireless services

18 Digital rights management and watermarking: An attack-localizing watermarking

 scheme for natural language documents
Gaurav Gupta, Josef Pieprzyk, Hua Xiong Wang
March 2006 **Proceedings of the 2006 ACM Symposium on Information, computer and communications security ASIACCS '06**

Publisher: ACM Press

Full text available:  pdf(390.28 KB) Additional Information: [full citation](#), [abstract](#), [references](#)

We present a text watermarking scheme that embeds a bitstream watermark W_i in a text document P preserving the meaning, context, and flow of the document. The document is viewed as a set of paragraphs, each paragraph being a set of sentences. The sequence of paragraphs and sentences used to embed watermark bits is permuted using a secret key. Then, English language sentence transformations are used to modify sentence lengths, thus embedding watermarking bits in the Least ...

Keywords: copyright, permutation, watermarking

19 Digital signets: self-enforcing protection of digital information (preliminary version)

Cynthia Dwork, Jeffrey Lotspiech, Moni Naor

 July 1996 **Proceedings of the twenty-eighth annual ACM symposium on Theory of computing**
Publisher: ACM Press
Full text available:  pdf(1.24 MB) Additional Information: [full citation](#), [references](#), [citations](#), [index terms](#)

20 Security: Efficient secure aggregation in VANETs 

 Maxim Raya, Adel Aziz, Jean-Pierre Hubaux
September 2006 **Proceedings of the 3rd international workshop on Vehicular ad hoc networks VANET '06**

Publisher: ACM Press

Full text available:  pdf(306.90 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

In VANETs, better communication efficiency can be achieved by sacrificing security and vice versa. But VANETs cannot get started without either of them. In this paper, we propose a set of mechanisms that can actually reconcile these two contradictory requirements. The main idea is to use message aggregation and group communication. The first class of solutions is based on asymmetric cryptographic primitives, the second class uses symmetric ones, and the third one mixes the two. We have also eval ...

Keywords: aggregation, efficiency, group communication, onion signature, security, vehicular networks

Results 1 - 20 of 200

Result page: **1** [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [next](#)

The ACM Portal is published by the Association for Computing Machinery. Copyright © 2006 ACM, Inc.

[Terms of Usage](#) [Privacy Policy](#) [Code of Ethics](#) [Contact Us](#)

Useful downloads:  [Adobe Acrobat](#)  [QuickTime](#)  [Windows Media Player](#)  [Real Player](#)